Annual Report to Congress on Foreign Economic Collection and Industrial Espionage: 1996

This report was prepared by the National Counterintelligence Center.

Table of Contents

Key Judgments

Updated information reaffirms the 1995 Annual Report. Contributors noted little new in the origin of the threat, collection targets, or methods used in effecting economic collection and industrial espionage.

Analysis of updated information reported by US counterintelligence (CI) agencies indicates that individuals, corporations, or government entities associated with at least 12 countries are assessed to be actively targeting US proprietary economic information and critical technologies. This includes all of the 10 countries previously identified in the 1995 *Annual Report.*

The 12 countries assessed to be actively collecting against US interests have shown particular determination, and in most cases a willingness to use illegal and covert means, to collect US economic and technological information.

Inquiries and investigations of suspicious incidents have increased significantly; there are tentative indications of an expansion of nontraditional collection targeting US industry.

Foreign collection continues to focus on economic and S&T information and products. US Defense investigators noted a primary focus on information systems technology. Foreign government and commercial collection continues to focus on dual-use technologies.

Overt, open-source, and legal collection methods are most evident, but reliance on illegal, covert, and traditional espionage methods has not abated. Analysis suggests venues of collection efforts may be in flux as communications proliferate and marketplace expansion continues. These developments will provide more opportunities to access targeted information and technologies in the United States and globally.

A special report released by the American Society for Industrial Security (ASIS) in March 1996 indicates that the loss of intellectual property is a growing problem for US business.

Background and Introduction

The *Intelligence Authorization Act for Fiscal Year 1995*, Section 809(b), requires that the President annually submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. This document updates the first *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage 1995*, which was released in July 1995.

For this first update, the Honorable Larry Combest, Chair of the House Permanent Select Committee on Intelligence (HPSCI), requested the following:

"Having considered the issue, we believe it is appropriate for the President to convey the update to Congress in letter form. We believe the letter should provide new information pertaining to or information significantly changing the portion of the original report describing the nature of the threat. To the extent practicable, the letter should be unclassified, accompanied by a classified annex, if appropriate."

On the basis of this 12 February 1996 Congressional request, Nora Slatkin, Chair of the National Counterintelligence Policy Board, tasked the National Counterintelligence Center (NACIC) to draft a community-based response. Accordingly, the NACIC requested the assistance of the following Executive Branch agencies to provide the data necessary to update the previous report:

Air Force Office of Special Investigations.

Central Intelligence Agency; Counterintelligence Center.

Defense Intelligence Agency.

Defense Investigative Service (DIS).

Department of Commerce; Office of Export Enforcement.

Department of Customs; Office of Intelligence.

Department of Energy; Counterintelligence Division.

Department of State; Bureaus of Intelligence and Research and Diplomatic Security.

Federal Bureau of Investigation (FBI); National Security Division.

Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; Director of Counterintelligence and Security Programs.

Naval Criminal Investigative Service.

National Security Agency.

US Army Intelligence and Security Command.

Input from each of these agencies has been incorporated into this report. Most offices responded, however, that they had no significant new information to report since last year's report. The FBI, CIA, and DIS cited numerous incidents over the past year of

continuing foreign economic collection and industrial espionage. While no new information was received that indicated a significant change in the assessed nature of the threat or the number of foreign countries assessed as most actively engaged in collection against US interests, the inputs clearly show such activity to be a continuing concern. The main body of this report addresses the nature of this concern and presents relevant findings and conclusions without identifying the specific countries involved. A listing of countries believed actively involved in targeting US economic and industrial interests is contained in a separate classified Annex B.

To underscore the level of national concern over this issue, on 28 February 1996, FBI Director Louis Freeh testified before a joint hearing of the Senate Judiciary and Intelligence Committees on the threat of economic espionage to the United States. FBI Director Freeh told the committees that he strongly supported a statute that would allow the US Government to better counter economic espionage against the US Government and US firms. In his unclassified prepared statement, FBI Director Freeh noted that the number of economic espionage cases under FBI investigation has continued to increase.

The three sections of this report correspond to the three aspects of threat required by Section 809(b) of the Intelligence Authorization Act of 1995 to be updated annually, which are specified in the original language from the Act :

Structure of the Report

The three sections of this report correspond to the three aspects of threat required by Section 809(b) of the Intelligence Authorization Act of 1995 to be updated annually, which are specified in the original language from the Act:

The threat to US industry of foreign industrial espionage and any trends in that threat, including:

The number and identity of the foreign governments conducting foreign industrial espionage.

The industrial sectors and types of information and technology targeted by such espionage.

The methods used to conduct such espionage.

This report updates the US Government's last report on "foreign industrial espionage" as specifically requested by Congress. It examines the full range of potentially damaging collection efforts against US national and corporate interests by foreign intelligence services, other government agencies, and private firms in two broad areas of concern-

economic intelligence collection and illicit acquisition of technological and other proprietary information.

To better identify and quantify the foreign-sponsored threats to private industry, this report also briefly refers to findings contained in a 1996 special report titled *Intellectual Property Theft and Corporate Espionage* based on a survey by the ASIS. Although not sponsored by the US Intelligence Community, this private-sector report provides valuable insight on the trends and risks associated with intellectual property protection and loss, as viewed by 325 individual US corporations. Summarized findings particularly relevant to this update are provided in Annex A.

Origin of the Threat

Report on the threat to US industry of foreign industrial espionage and any trends in that threat, including the number and identity of the foreign governments conducting foreign industrial espionage.

During the past year, the US CI community has identified activities of individuals, corporations, or government entities from at least 12 countries that are most frequently the subjects of reports, allegations, and conclusive investigations for suspected economic and industrial espionage activity. These countries are assessed to be the most aggressive and deliberate in collection efforts directed against US proprietary economic information and critical technologies. They have shown particular determination, and in most cases a willingness to use illegal and covert means, to collect against US interests.

In addition, reporting agencies, particularly the FBI and DIS, cited a substantial number of suspicious incidents and investigations potentially involving economic espionage or industrial intelligence collection. While these reported incidents involve a diverse assortment of entities and an additional 26 foreign countries, outcomes of these investigations are pending, and no conclusive judgments are possible at this time.

Those entities assessed to be actively targeting US persons, firms, industries, and US Government activities do so in order to steal or wrongfully obtain critical technologies, data, and information. The increasing value of proprietary economic information in the global and domestic marketplaces, greater access to the "information superhighway," and the proliferation of new technology demands combine to increase both the opportunities and motives for conducting economic collection and industrial espionage.

In the area of US defense-industry reporting of suspicious activity, DIS and some of the military CI agencies reported continued low-level collection interest and activity by foreign companies and governments. For example, in 1995 some 249 CI issues were referred to DIS personnel by cleared Department of Defense (DOD) contractors and were

significant enough for DIS to in turn refer them to appropriate US CI agencies. Incidents cited by DIS included nine of the 10 countries reported by NACIC in the initial 1995 Annual Report and closely paralleled updated information submitted by the FBI and CIA. Updated incidents cited by Navy and Air Force CI components were also consistent with data reported by FBI and CIA. Other suspicious incident reporting from DIS involved an additional 17 foreign countries; referrals, investigations, and analysis of these data are ongoing.

In 1996, the FBI and ASIS also reaffirmed the increase in the reporting of domestic theft or misappropriation of proprietary economic information. An ASIS special report released in March 1996, *Trends in Intellectual Property Loss,* indicated that 74 percent of intellectual or proprietary property losses stemmed from the actions of "trusted relationships"-employees, former employees, contractors, suppliers, and so forth. More relevant for this update is the fact that participants in the ASIS survey also attributed losses to foreign competitors, foreign intelligence services, and foreign business partners. Some additional findings from this study are presented later in this section.

Through its Economic Counterintelligence Program, the FBI has developed significant information on the foreign economic threat-including the identification of the foreign governments who conduct foreign industrial espionage. In his 28 February 1996 statement before the Senate Judiciary and Intelligence Committees, FBI Director Freeh stated that, since the initiation of the FBI's Economic Counterintelligence Program in 1994, the FBI has observed a 100-percent increase in the number of suspected economic espionage cases currently under investigation-from 400 to 800 cases.

It should be noted that FBI investigations dramatically increased during the past year primarily because of recent changes in the FBI's CI program and because of its concomitant dedication of more resources and initiatives to deal with this serious economic problem. Because the data reported stem from greater FBI emphasis and resources directed at the problem, the increase in the total number of ongoing cases does not necessarily indicate a trend that will prove to increase each year nor can it be assumed that each case will prove conclusively to be a valid instance of economic espionage or industrial collection. The surge in investigations suggests a great number of suspicious incidents. Because the FBI designated additional resources to investigate these types of cases, the increase in cases may indicate a longstanding problem only now being accurately defined. (In a related development, DIS reported an expectation of improved incident data concerning suspected activities as a result of better security education and standardized reporting.)

The increased number of current FBI investigations of suspected economic espionage encompasses 23 foreign countries-traditional adversaries and allies-and 12 of the countries are the same as those assessed by the NACIC as most actively targeting US economic and industrial interests. Significantly, 11 of these 12 countries are the basis for over 90 percent of the FBI's current investigations into economic espionage activities;

these countries are the highest priority targets of its new Economic Counterintelligence Program.

Overall, CI community inputs and NACIC analysis of all relevant available information revealed considerable consistency in both raw data and conclusions. These aggregated data were consistent also with the 1995 *Annual Report*. Most significant, contributors uniformly reaffirmed the threat assessment presented in the previous *Annual Report*.

Assuming reasonably accurate and deconflicted input, coupled with conservative CI analytic judgments, the number of foreign countries assessed to be most actively targeting US information appears not to have changed significantly. The number of such countries has increased slightly, from 10 to 12, since the last *Annual Report* in 1995. These 12 countries do not necessarily reflect the full picture of targeting against US economic interests. Since economic collection and industrial espionage are complex issues, some types of collection do not constitute illegal behavior. In some instances, however, suspicious incidents could be precursors to illicit collection activities or indicate the intelligence interests of foreign powers. Furthermore, note should be made of the current large number of incidents for which investigations and eventual analysis of the outcome remain to be accomplished.

FBI, CIA, and DIS each provided updates that essentially reaffirmed the 1995 *Annual Report* findings in terms of countries involved in targeting US proprietary economic information and critical technologies. New inputs from the military CI components were also consistent with those from non-Defense agencies. It was evaluation of these data, in toto, that resulted in a total number increase from 10 to 12 countries.

ASIS findings on the nature and scope of reported losses from economic collection or industrial espionage generally parallel the assessed threat as presented by the US CI community. In its March 1996 report, *Trends in Intellectual Property Loss*, ASIS named eight of the same 12 countries identified by the US CI community as either participants or localities in instances where attempts were made to collect US proprietary economic information. Interestingly, of all the foreign localities or nationalities for incidents reported by ASIS, there was a 75-percent correlation with reported investigative activities by the FBI and a 68-percent correlation with incident referrals identified by DIS. While not an exact overlay, these data generally corroborate the data and findings combined from official US Intelligence Community and law enforcement agencies.

One unique aspect of the private-sector survey, seldom available in CI community assessments, was the magnitude of the estimated dollar loss from economic spying-potentially $2 billion a month for all US businesses. A summary of findings of the ASIS special report particularly relevant to this update is provided in Annex A.Report on the threat to US industry of foreign industrial espionage and any trends in that threat, including the industrial sectors and types of information and technology targeted by such espionage.

Targeted Information and Technology

Report on the threat to US industry of foreign industrial espionage and any trends in that threat, including the number and identity of the foreign governments conducting foreign industrial espionage.

Foreign collection continues to focus on economic and S&T information and products. Both foreign government and foreign commercially sponsored collection activities consistently target dual-use technologies. Although traditional foreign threat countries continue their collection activities, reporting indicates the expansion of nontraditional foreign threat collection within US industry.

According to the FBI and DIS, high-technology and defense-related industries remain the primary targets of foreign economic intelligence collection operations. This finding continues a trend reported in the 1995 *Annual Report*. The most likely industry targets of economic espionage and other collection activities during the past year include the following areas, most of which are included on the 1996 Military Critical Technology List (MCTL):

Advanced materials and coatings.

Advanced transportation and engine technology.

Aeronautics systems.

Aerospace.

Armaments and energetic materials.

Biotechnology.

Chemical and biological systems.

Computer software and hardware.

Defense and armaments technology.

Directed and kinetic energy systems.

Electronics.

Energy research.

Guidance, navigation, and vehicle control.

Information systems.

Information warfare.

Manufacturing and fabrication.

Manufacturing processes.

Marine systems.

Materials.

Nuclear systems.

Semiconductors.

Sensors and lasers.

Signature control.

Space systems.

Telecommunications.

Weapons effects and countermeasures.

According to a DIS summary of suspicious contacts reported in FY 1995, entities associated with 26 foreign countries displayed an interest in 16 of the 18 technology categories listed in the newest MCTL. The United States considers all the above industries to be strategically important because they produce classified products for the government, produce dual-use technology used in both the public and private sectors, or are responsible for the leading-edge technologies required to maintain US economic security.

FBI Director Freeh provided the following five examples of foreign targeting activities in his 28 February 1996 statement before the Senate Judiciary and Intelligence Committees:

One foreign-government-controlled corporation targeted US proprietary business documents and information from US telecommunications competitors.

Another foreign competitor acquired the technical specifications from a US automotive manufacturer.

In violation of US export laws, a foreign company attempted to acquire a US company's restricted radar technology.

Several US companies reported the targeting and acquisition of proprietary biotechnology information.

One US company reported the foreign theft of its manufacturing technology regarding its microprocessors.

In addition to revealing collection efforts against technological information, both FBI and DIS reporting continue to reflect an increasing trend of foreign collection activity against US Government economic policy information. These collection efforts seek to obtain advance knowledge about US policy guidelines, negotiations, and proposals in order to give the foreign country an added advantage in bilateral or international negotiations. Types of US Government economic information- especially prepublication or unpublished "insider" data-of special interest to foreign governments and intelligence services include:

Bid proposals.

Economic, trade, and financial agreements.

Energy policies.

Marketing plans.

Price structuring.

Proposed legislation affecting the profitability of foreign firms operating in the United States.

Tax and other monetary policies.

Technology transfer and munitions control regulations.

Trade developments.

Collection Methods

Report on the threat to US industry of foreign industrial espionage and any trends in that threat, including the number and identity of the foreign governments conducting foreign industrial espionage.

The collection methods utilized by foreign governments to gather information on economic matters remain largely unchanged from last year's report. Traditional espionage

methods-once primarily reserved for collecting US national defense information-continue to be applied to the collection of economic and proprietary information.

Practitioners of economic espionage seldom use one method of collection; rather, their concerted collection programs combine both legal and illegal, traditional, and more innovative methods. FBI investigations continue to identify the various methods utilized by those engaged in economic espionage. In addition, the FBI continues to assess the scope of coordinated intelligence efforts against the United States.

DIS reported that foreign economic collection methodology continues to present various security countermeasures concerns to the defense industry. Foreign intelligence services still use clandestine means, but foreign governments also rely significantly on overt and perfectly legal collection methods.

Foreign collectors are known to use accessible databases and information systems, including the Internet, to identify and target information. This methodology is not limited to foreign commercially sponsored activity, but also includes foreign intelligence service operations.

Worldwide connectivity of information systems and global marketing ventures create a complex and varied target environment for collectors.

Because of the growing popularity and expansion of the Internet, the US defense industry reports significant increases in security countermeasures incidents associated with computer-based collection attempts. Large amounts of DOD technical information are transferred over the Internet on a daily basis and could be targeted by hostile entities. Corporate America has an even greater presence on publicly accessible networks. The Internet and E-mail networks provide direct methods of exploitation for foreign collection efforts. This is of particular concern in situations where programs to monitor the content of such online communications are lacking, and access can be gained through public gateways or hacking techniques. Access to a company's bulletin board and home page on the Internet, internal E-mail, and employees may provide foreign collectors with many avenues to broaden their collection efforts.

Annex A

ASIS Special Report: Trends in Intellectual Property Loss

The American Society for Industrial Security (ASIS) issued a special report in March 1996 titled *Trends in Intellectual Property Loss.*

Because the US Government does not keep statistics on private-industry losses, the ASIS survey provides valuable insight into corporate America's self-assessment of the trends and risks associated with intellectual property protection. ASIS reported incidents by a variety of categories ranging from frequency and types of industry to localities of incidents and reported nationality of those involved. For example, ASIS reported incidents associated with 16 nationalities or countries; eight of the named countries were among the 12 countries assessed by the US counterintelligence community to be most actively involved in targeting US interests.

The ASIS report presents data that indicate some foreign companies and governments pose a significant and continuing threat to intellectual property-which the report's authors defined as patents, copyrights, trademarks, and trade secrets-and that such activity will have mounting negative effects on US industry.

Findings particularly relevant to National Counterintelligence Center's 1996 updated *Annual Report*, as presented in the ASIS report, are presented below:

Reported incidents increased 323 percent since 1992. Losses of corporate information increased from a reported 9.9 incidents per month in 1992 to an average of 32 incidents per month in 1995.

About three-fourths of reported losses occurred in the United States, and the majority of those incidents involved "trusted relationships" (employees, vendors, contractors, retirees, and so forth).

Other incidents were attributable to a variety of sources: domestic competitors, computer hackers, foreign competitors, foreign intelligence services, and foreign business partners.

Of incidents outside the United States, approximately half took place in countries traditionally considered allies of the United States.

Foreign nationals were identified in 21 percent of the incidents where the perpetrator's nationality was known.

The prepublication copy of the ASIS report reviewed by the NACIC totaled 35 pages of text and charts, and presented numerous other findings that summarized contributors' views on incidents and losses affecting American-based companies. In the report, the responding companies surveyed are broken out into three categories-"Services," "High-Tech," and "Manufacturing" - and most of the survey data is grouped and discussed from these categories. Included are general and specific discussion areas that cover incidents and losses by category; incidents by locality and nationality; methods of acquisition/collection; impact of losses by category; and the essential content and implementation of formal industry programs for safeguarding proprietary information. The report's authors comment in their conclusions:

". . . we must act decisively. Corporate management has a fiduciary responsibility to stockholders to take reasonable and prudent steps to safeguard intellectual property assets."